CLAIMS

What is claimed is:

1   1. A method of deterring a rollback attack against a first database
2   comprising:
3   determining if the first database is corrupted, the first database being
4   associated with a first authentication code;
5   determining if a second database is corrupted when the first database is
6   corrupted, the second database being associated with a second authentication
7   code, the second database having contents substantially the same as the first
8   database;
9   when the second database is not corrupted, recalculating the second
10 authentication code using a portion of the first authentication code, copying the
11 second database over the first database, and proceeding with authorized
12 operations for processing content by an application program.
13

1   2. The method of claim 1, when the second database is not corrupted,
2   further comprising presenting a challenge code to a user of the application
3   program, requiring the user to obtain a passcode in response to the challenge
4   code, and determining validity of the passcode, and performing the recalculating
5   and copying only when the passcode is valid.
6

1   3. The method of claim 1, further comprising continuing with authorized
2   operations of the application program for processing content when the first
3   database is not corrupted.
4

1   4. The method of claim 1, wherein the first database comprises usage
2   rules for processing selected content by the application program, the usage rules
3   including a copy count for the selected content.
4

1   5. The method of claim 1, wherein the content comprises digital audio
2   data.
3

1   6. The method of claim 5, wherein the application program complies with
2   requirements for a secure digital music initiative (SDMI) implementation.
3

1   7. The method of claim 1, wherein the first authentication code comprises
2   a hash of the first database and a first secret, and the second authentication
3   code comprises a hash of the second database and a second secret, the first
4   secret being different than the second secret.
5

1   8. The method of claim 7, wherein the portion comprises the first secret.

2

1   9. The method of claim 2, further comprising allowing a predetermined
2   number of operations of copying the second database over the first database
3   without presenting a challenge code to the user, requiring the user to obtain the
4   passcode, and determining the validity of the passcode.
5

1   10. An article comprising: a storage medium having a plurality of machine
2   readable instructions, wherein when the instructions are executed by a
3   processor, the instructions provide for deterring a rollback attack against a first
4   database by determining if the first database is corrupted, the first database
5   being associated with a first authentication code, by determining if a second
6   database is corrupted when the first database is corrupted, the second database
7   being associated with a second authentication code, the second database
8   having contents substantially the same as the first database, and when the
9   second database is not corrupted, recalculating the second authentication code
10   using a portion of the first authentication code, copying the second database
11   over the first database, and proceeding with authorized operations for processing
12   content by an application program.
13

1   11. The article of claim 10, when the second database is not corrupted,

2   further comprising instructions for presenting a challenge code to a user of the

3   application program, for requiring the user to obtain a passcode in response to

4   the challenge code, and for determining validity of the passcode, and for

5   performing the recalculating and copying only when the passcode is valid.

6

1   12. The article of claim 10, further comprising instructions for continuing

2   with authorized operations of the application program for processing content

3   when the first database is not corrupted.

4

1   13. The article of claim 10, wherein the first database comprises usage

2   rules for processing selected content by the application program, the usage rules

3   including a copy count for the selected content.

4

1   14. The article of claim 10, wherein the content comprises digital audio

2   data.

3

1   15. The article of claim 14, wherein the application program complies with

2   requirements for a secure digital music initiative (SDMI) implementation.

3

1   16. The article of claim 10, wherein the first authentication code

2   comprises a hash of the first database and a first secret, and the second

3   authentication code comprises a hash of the second database and a second

4   secret, the first secret being different than the second secret.

5

1   17. The article of claim 16, wherein the portion comprises the first secret.

2

1   18. The article of claim 11, further comprising instructions for allowing a

2   predetermined number of operations of copying the second database over the

3   first database without presenting a challenge code to the user, requiring the user

4   to obtain the passcode, and determining the validity of the passcode.

17

5

1   19. A method of deterring circumvention of a content protection system of

2   an application program via restoration of a first control database, the first control

3   database being associated with the application program and including usage

4   rules for digital audio content, comprising:

5   determining if the first control database is corrupted, the first control

6   database being associated with a first message authentication code (MAC);

7   determining if a second control database is corrupted when the first

8   control database is corrupted, the second control database being associated with

9   a second message authentication code (MAC), the second control database

10   having contents substantially the same as the first control database;

11   when the second control database is not corrupted, performing the

12   following actions:

13   presenting a challenge code to a user of the application program;

14   requiring the user to obtain a passcode in response to the

15   challenge code; and

16   determining validity of the passcode;

17   recalculating the second MAC using a portion of the first MAC and

18   copying the second control database over the first control database when

19   the passcode is valid; and

20   proceeding with authorized operations for processing the digital

21   audio content by an application program consistent with the usage rules.

22

1   20. The method of claim 19, wherein the usage rules comprise a copy

2   count for the digital audio content.

3

1   21. The method of claim 20, wherein the application program complies

2   with requirements for a secure digital music initiative (SDMI) implementation.

3

1   22. The method of claim 19, wherein the first MAC comprises a hash of

2   the first control database and a first secret, and the second MAC comprises a

3 hash of the second control database and a second secret, the first secret being

4 different than the second secret.

5

1   23. The method of claim 19, further comprising allowing a predetermined

2 number of operations of copying the second control database over the first

3 control database without presenting a challenge code to the user, requiring the

4 user to obtain the passcode, and determining the validity of the passcode.

5

1   24. The method of claim 19, wherein copying of the second control

2 database over the first control database is performed after beginning execution

3 of the application program but before proceeding with authorized operations for

4 processing the digital audio content by an application program consistent with

5 the usage rules.

1   25. An article comprising: a storage medium having a plurality of machine

2 readable instructions, wherein when the instructions are executed by a

3 processor, the instructions provide for deterring circumvention of a content

4 protection system of an application program via restoration of a first control

5 database, the first control database being associated with the application

6 program and including usage rules for digital audio content, by

7   determining if the first control database is corrupted, the first control

8 database being associated with a first message authentication code (MAC);

9   determining if a second control database is corrupted when the first

10 control database is corrupted, the second control database being associated with

11 a second message authentication code (MAC), the second control database

12 having contents substantially the same as the first control database;

13   when the second control database is not corrupted, performing the

14 following actions:

15   presenting a challenge code to a user of the application program;

16   requiring the user to obtain a passcode in response to the

17   challenge code; and

18   determining validity of the passcode;

19	recalculating the second MAC using a portion of the first MAC and
20	copying the second control database over the first control database when
21	the passcode is valid; and
22	proceeding with authorized operations for processing the digital
23	audio content by an application program consistent with the usage rules.
24	

1	26. The article of claim 25, wherein the usage rules comprise a copy
2	count for the digital audio content.
3	

1	27. The article of claim 25, wherein the first MAC comprises a hash of the
2	first control database and a first secret, and the second MAC comprises a hash
3	of the second control database and a second secret, the first secret being
4	different than the second secret.
5	

1	28. The article of claim 25, further comprising instructions for allowing a
2	predetermined number of operations of copying the second control database
3	over the first control database without presenting a challenge code to the user,
4	requiring the user to obtain the passcode, and determining the validity of the
5	passcode.
6	
7	